What is Claimed is:

1. A universal crypto-adaptor system for supporting one or more smartcard applications with a plurality of smart cards through a smart card reader, comprising:

means for providing implementations of API specification for said smartcard applications; and

a universal smart card API for communicating with said API means and said smart card reader for handling smart card operations including file and data managements and cryptographic operations, wherein said universal smart card comprises at least a smartcard translator to retrieve and translate smart card data saved in said respective smart card into a plurality of logic partitions that are compatible with each of said smartcard applications of said API means.

2. The system, as recited in claim 1, wherein said smartcard applications include CSP (Microsoft Cryptographic Application Interface) applications and a PKCS11 (Cryptographic Token Interface Standard from RSA Security) applications.

3. The system, as recited in claim 2, wherein said smart cards include WPC card, SCT card and Java card.

4. The system, as recited in claim 3, wherein said API means includes a CSP component which is a CSP API specification that implements a CSP context and context policies and a PKCS11 component which is a PKCS API specification that implements a PKCS session, a crypto slot and a PKCS object management.

5. The system, as recited in claim 4, wherein said universal smart card API comprises at least a WPC smartcard translator, a SCT smartcard translator, and a Java card smartcard translator corresponding to said WPC card, said SCT card and said Java card respectively.

6. The system, as recited in claim 5, wherein said universal crypto-adaptor system further supports cryptographic operations, including a RSA private key

encryption or signing and a DES encryption and decryption by defining a vendor PKCS object attribute, CKA_DONTDORSA.

7. The system, as recited in claim 1, wherein said universal smart card API splits said smart card data received from said smart cards into said logic partitions, wherein each of said partitions is a slot to store said smart card data of different information from said smart cards.

8. The system, as recited in claim 7, wherein universal smart card API includes at least a Slot 0 as a master slot that contains cardholder information, a rest each Slot is for each identity or application, a Slot 1 for credit card data, and a Slot 2 for health insurance data. Generally, each slot has said same type data but different data.

9. The system, as recited in claim 6, wherein said universal smart card API splits said smart card data received from said smart cards into said logic partitions, wherein each of said partitions is a slot to store said smart card data of different information from said smart cards.

10. The system, as recited in claim 9, wherein universal smart card API includes at least a Slot 0 as a master slot that contains cardholder information, a rest each Slot is for each identity or application, a Slot1 for credit card data, and a Slot 2 for health insurance data. Generally, each slot has said same type data but different data.

11. The system, as recited in claim 6, wherein when said smart card data is retrieved from said smart card, said smartcard translator converts TLV into PKCS11 object attributes and creates said PKCS11 object while said PKCS11 object attribute is also in TLV format.

12. The system, as recited in claim 8, wherein when said smart card data is retrieved from said smart card, said smartcard translator converts TLV into PKCS11 object attributes and creates said PKCS11 object while said PKCS11 object attribute is also in TLV format.

13. The system, as recited in claim 10, wherein when said smart card data is retrieved from said smart card, said smartcard translator converts TLV into PKCS11

object attributes and creates said PKCS11 object while said PKCS11 object attribute is also in TLV format.

14. A method of incorporating a smart card with a cryptographic application, comprising the steps of:

(a) checking for a smart card;

(b) requesting and receiving a smart card ATR (Answer To Reset string) from said smart card when said smart card is found;

(c) selecting a smartcard translator correspondingly, depending on said card ATR;

(d) searching public data on said smart card and creating a public application object correspondinly by said smartcard translator, such as a PKCS11 object or a CSP object;

(e) receiving a password from a smartcard application, such as CSP application or PKCS11 application, and sending said password to said selected smartcard translator for sending said password to said smart card for confirmation;

(f) searching private key object on said smart card and creating private application objects correspondingly by said smartcard translator;

(g) searching said private key object on said smart card for confirmation;

(h) receiving a function command with a private key object handle and data from said smartcard application by using said private key object handle and forwarding said data to said smart card with specifying a specific file name for executing a specific function, wherein said smartcard translator gets an attribute from said private key object so that said smartcard translator knows how to access a key file on said smart card; and

(i) receiving said data executed from said smart card and returning to said smartcard application.

15. The method, as recited in claim 14, wherein when said function is signing function, said function command is a signing command and said data forwarded to said smart card from said smartcard application in the step (h) is signed by said smart card and returned to said smartcard application through said universal crypto-adaptor system.

16. The method, as recited in claim 14, further comprising a step of saving said data in a "Type, Length and Value" (TLV) format.